

J. Paul Gignac (CSB# 125676)
Helen Kim (CSB# 260195)
ARIAS OZZELLO & GIGNAC LLP
115 South La Cumbre Lane, Suite 300
Santa Barbara, California 93105
Telephone: (805) 683-7400
Facsimile: (805) 683-7401
j.paul@aogllp.com
hkim@aogllp.com

ADR

Filed

DEC 23 2011

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

Peter J. Bezek (CSB# 102310)
Robert A. Curtis (CSB# 203870)
FOLEY BEZEK BEHLE & CURTIS LLP
15 West Carrillo Street
Santa Barbara, California 93101
Telephone: (805) 962-9495
Facsimile: (805) 962-0722
pbezek@foleybezek.com
rcurtis@foleybezek.com

E-filing

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

MATTHEW HILES, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

CARRIER IQ, INC., a Delaware
corporation; LG ELECTRONICS, INC., a
South Korea corporation; LG
ELECTRONICS USA, INC., a Delaware
corporation; and DOES 1 through 100,

Defendants.

Case No. CV 11-06641

PSG

CLASS ACTION COMPLAINT FOR:

- (1) VIOLATION OF THE FEDERAL
WIRETAP ACT, 18 U.S.C. §2511;
- (2) DECLARATORY RELIEF UNDER THE
DECLARATORY JUDGMENT ACT, 28
U.S.C. §2201;
- (3) VIOLATION OF CALIFORNIA BUSINESS
AND PROFESSIONS CODE § 17200; AND
- (4) INVASION OF PRIVACY.

DEMAND FOR JURY TRIAL

ORIGINAL

1 All allegations in this Complaint, other than those allegations in paragraphs 8 and 62
2 through 66 that are specific to plaintiff Matthew Hiles ("Plaintiff"), are based upon information
3 and belief. Plaintiff's information and belief are based upon, *inter alia*, Plaintiff's own
4 investigation and the investigation conducted by Plaintiff's attorneys. Each allegation in this
5 Complaint either has evidentiary support or, alternatively, is likely to have evidentiary support
6 after a reasonable opportunity for further investigation and/or discovery.

7 NATURE OF THE ACTION

8 1. This case is a nationwide class action, on behalf of Plaintiff and all other
9 similarly situated persons, seeking, *inter alia*, declaratory and injunctive relief, statutory
10 penalties and/or damages, attorneys' fees and other relief. This case arises out of the actions of
11 defendants Carrier IQ, Inc., LG Electronics, Inc., and LG Electronics USA, Inc. ("Defendants").
12 Defendants have designed and installed software called IQ Agent on millions of cell phones and
13 other mobile devices across the country. IQ Agent records and transmits to cellular carriers,
14 such as Sprint and AT&T, data relating to customers' cellular phone use. The data is then
15 analyzed by the carriers and used for a variety of undisclosed purposes. IQ Agent cannot be
16 removed from cell phones and cannot be readily detected by cell phone owners. Moreover, cell
17 phone owners are not notified of its presence; nor are they asked to agree to its operation.

18 2. Published research into IQ Agent's functionality reveals that the software records
19 numerous types of information for transmission to Carrier IQ's carrier customers, including the
20 path of web addresses meant to be transmitted securely via the HTTPS protocol between cell
21 phone users and the web servers they visit. Thus, IQ Agent intercepts electronic
22 communications that cell phone users intend to be "secure" (e.g., bank account numbers, user
23 names, passwords and search terms). Because Carrier IQ's software intercepts and transmits
24 private electronic communications and other electronic information, Defendants' use of IQ
25 Agent to obtain such information from consumers violates, *inter alia*, the Federal Wiretap Act,
26 18 U.S.C. § 2511, *et seq.* Defendants' use of IQ Agent also constitutes an invasion of privacy
27 and unfair competition under California law.
28

1 3. The relief that Plaintiff seeks in this action is primarily equitable in nature in that
2 Plaintiff seeks declaratory and injunctive relief that will result in: (a) Defendants being enjoined
3 from intercepting, disclosing and/or using any and all electronic and/or wire communications by
4 means of the IQ Agent software; (b) Defendants disposing of or destroying the wire and/or
5 electronic communications intercepted by Defendants that belong to Plaintiff and the class
6 members; and (c) IQ Agent being deactivated or removed from all LG mobile devices or all LG
7 mobile devices installed with IQ Agent being replaced with the same LG mobile devices without
8 IQ Agent installed on them.

9
10 **JURISDICTION AND VENUE**

11 4. This Court has subject matter jurisdiction over the claims alleged herein pursuant
12 to 28 U.S.C. § 1331.

13 5. This Court has supplemental jurisdiction over the California state law claims
14 alleged herein pursuant to 28 U.S.C. § 1367(a) because those claims are so related to the federal
15 law claims alleged that they form part of the same case or controversy under Article III of the
16 United States Constitution.

17 6. Venue in this judicial district is proper under 28 U.S.C. § 1391 because defendant
18 Carrier IQ, Inc. is headquartered in this judicial district, because the conduct complained of
19 emanated from within this judicial district, and because the claims alleged in this action arise, at
20 least in part, in this judicial district.

21 **INTRADISTRICT ASSIGNMENT**

22 7. Venue is proper in the San Jose division of this judicial district under Local
23 Rule 3-2(c) because a substantial part of the events or omissions which give rise to the claims
24 alleged herein occurred in the San Jose judicial district.

25 **PARTIES**

26 8. Plaintiff Matthew Hiles resides in Davenport, Iowa. Plaintiff owns an LG
27 Marquee Smartphone that uses the Google Android operating system and on which the IQ Agent
28 software is installed.

10. Defendant LG Electronics, Inc. ("LG, Inc.") is a foreign corporation with its principal place of business located in Seoul, South Korea. LG, Inc. designs and manufactures mobile devices known as "Smartphones", including Plaintiff's LG Marquee Smartphone. LG, Inc. is the parent company of LG Electronics USA, Inc.

11. Defendant LG Electronics USA, Inc. (“LG USA”) is a Delaware corporation with its principal place of business located in Englewood Cliffs, New Jersey. LG USA sells and distributes Smartphones throughout the United States, including Plaintiff’s LG Marquee Smartphone.

12. Plaintiff does not know the true names and capacities of DOES 1 through 100, inclusive, whether individual, corporate, associate or otherwise and, therefore, sues said defendants, and each of them, by such fictitious names. Plaintiff will amend this Complaint to include their true names and capacities when they have been ascertained. DOES 1 through 100 are other parties that are in some manner legally responsible for the events, happenings and wrongdoing alleged in this Complaint.

13. As used herein, “Defendants” shall mean and refer to Carrier IQ, LG, LG USA and DOES 1 through 100, collectively, and “LG Defendants” shall mean and refer to LG, Inc., LG USA and DOES 51 through 100, collectively.

25 I. Carrier IQ Sells Its Software “IQ Agent” To Cellular Carriers And Mobile Phone Manufacturers So They Can Track And Analyze Users’ Experiences.

27 14. Carrier IQ has been operating since 2005 as a provider of software for cellular
carriers and mobile phone manufacturers.

1 15. Carrier IQ offers its customers, as its motto claims, “The Power of Knowing.” Its
2 software is now installed on more than 140 million mobile devices worldwide.

3 16. Carrier IQ states on its website that it has grown to become the “market leader in
4 Mobile Service Intelligence solutions that have revolutionized the way mobile operators and
5 device vendors gather and manage information from end users.”

6 17. Carrier IQ sells its “Mobile Service Intelligence” solutions to mobile phone
7 manufacturers and cellular service providers. On its website, the company touts its “unique
8 ability to provide detailed insight into service delivery and user experience.” Carrier IQ
9 promises its customers: “you can achieve your strategic goals more efficiently and effectively,
10 based on data drawn directly from your subscribers’ devices — the place where your customer
11 actually experiences the service.”

12 18. Carrier IQ’s Mobile Service Intelligence solution relies on its “unique ability to
13 analyze in detail usage scenarios and fault conditions by type, location, application and network
14 performance.”

15 19. Carrier IQ’s flagship product is its Mobile Service Intelligence Platform (MSIP),
16 which “receives raw data (known as Metrics) from phones and converts them into reliable,
17 repeatable Measures which feed into analytic applications.”

18 20. In particular, Carrier IQ’s “Insight Experience Manager uses data directly from
19 the mobile phone itself to give a precise view of how users interact with both their phones and
20 the services delivered through them, even if the phone is not communicating with the network.”

21 21. Carrier IQ states that its Insight Experience Manager will allow carriers or
22 manufacturers to “[i]dentify exactly how your customers interact with services and which ones
23 they use. See which content they consume, even offline.” Carriers and manufacturers can “view
24 application and device feature usage, such as camera, music, messaging, browser and TV.”

25 **II. Carrier IQ’s Previously Hidden Software “IQ Agent” Was Recently Discovered,**
26 **Causing A Public Outcry Over Its Impact On Consumer Privacy.**

27 22. In mid-November 2011, mobile developer Trevor Eckhart published a report on
28 his website detailing his discovery of a piece of software running on his HTC Smartphone called

1 IQ Agent. Eckhart raised questions regarding what function IQ Agent serves and what
2 information it has access to in its normal operation.

3 23. Eckhart discovered that IQ Agent is a hidden, irreplaceable, permanent piece of
4 software. Unlike all other applications and services on the Android operating system, IQ Agent
5 cannot be identified, terminated or removed without advanced computer and development skills.

6 24. Based on his initial investigation, Eckhart concluded that IQ Agent is a “rootkit,”
7 defined by Wikipedia as “software that enables continued privileged access to a computer while
8 actively hiding its presence from administrators by subverting standard operating system
9 functionality or other applications Although rootkits can serve a variety of ends, they have
10 gained notoriety primarily as malware, hiding applications that appropriate computing resources
11 or steal passwords without the knowledge of administrators and users of affected systems.”

12 25. Following Eckhart’s initial report, Carrier IQ sent Eckhart a cease and desist
13 letter demanding that he retract his description of the IQ Agent software as a “rootkit.”

14 26. The Electronic Frontier Foundation (EFF), which advocates for the freedom of
15 speech and openness in the technology field, responded on behalf of Eckhart, and Carrier IQ
16 quickly withdrew its demand. However, the conflict between Eckhart and Carrier IQ sparked
17 public interest. Eckhart then decided to further investigate the IQ Agent software.

18 27. The result of Eckhart’s investigation was a seventeen minute video, posted on
19 YouTube and his website, illustrating in detail how IQ Agent interacts with his HTC
20 Smartphone. The video can be found at http://www.youtube.com/watch?v=T17XQI_AYNo
21 (last accessed December 5, 2011). The video details IQ Agent’s functionality within the Google
22 Android operating system on Eckhart’s HTC Smartphone. Eckhart concludes that IQ Agent
23 functions more or less identically on other manufacturers’ Android phones as well.

24 28. Eckhart’s video sparked extensive public interest in the previously unknown IQ
25 Agent software and the company (Carrier IQ) that created it. Thousands of articles and blog
26 posts have examined Eckhart’s video and the potential impact of a piece of hidden software
27 having access to users’ sensitive information.
28

29. For example, the technology website *Gizmodo* (gizmodo.com) has published numerous articles relating to Carrier IQ and IQ Agent. Its initial article was headlined “Your Android Phone is Secretly Recording Everything You Do,” accompanied by a graphic stating “YOUR PHONE IS WATCHING YOU” and the picture of a phone with a hole through which an unidentified man is watching the user.

30. Public interest in Carrier IQ has also led to an informal U.S. Senate inquiry from Senator Al Franken, who sent Carrier IQ a letter expressing concern over its IQ Agent software’s impact on consumer privacy and requesting more information.

31. Numerous websites have published information on how owners of Android operating system cell phones and mobile devices can check to see if IQ Agent is installed on their cell phones and mobile devices.

III. IQ Agent Intercepts User Information And Transmits It To Cellular Carriers, Including Information That Is Meant To Be Secure And Encrypted Because It May Contain Sensitive Information.

32. Following the initial public outcry over the discovery of IQ Agent, researcher Dan Rosenberg investigated the internal functioning of the IQ Agent software.

33. Rosenberg uncovered a list of “metrics” that IQ Agent records without users’ knowledge. These metrics are captured and then transmitted to Carrier IQ’s carrier customers such as AT&T and Sprint, or to Carrier IQ’s servers.

34. Rosenberg confirmed that IQ Agent operates in the background of Android devices at all times, situated between the user and the operating system. The software logs extensive amounts of information about users’ experiences, including but not limited to:

- when users turn their mobile devices on or off;
- which applications users download, open and close;
- which applications crash on users’ devices;
- where users’ devices are located;
- whether calls or text messages are received by users;
- which websites users visit;
- whether the websites users visit load properly;

- whether users' screens are on or off;
- which keys users press on the phone dialer, even if the phone numbers are not dialed;
- user devices' battery level, voltage and temperature; and
- users' passwords and other private information entered into websites, including encrypted websites with the HTTPS prefix.

35. The most troubling of Rosenberg's discoveries is that IQ Agent, because it functions as a rootkit, intercepts communication between the internet browser and the web server a user visits, even when the user visits a website secured by the HTTPS internet protocol.

36. The HTTPS protocol allows users to enter sensitive information such as passwords into their internet browsers, and it sends it to the web servers they visit via an encrypted method. It is represented by the "https://" prefix as opposed to the standard "http://" prefix at the beginning of a web address. For example, Bank of America's secure online banking portal can be accessed at <https://www.bankofamerica.com>. When users type <http://www.bankofamerica.com>, they are automatically re-routed to the secure "https://" website.

37. The HTTPS protocol is commonly used in transactions that involve sensitive information such as credit card numbers, bank account numbers, usernames and passwords. The HTTPS protocol makes it impossible for external parties to intercept the traffic between users and the websites they visit because it encrypts the data exchanged between them. Consequently, users believe that they can shop online, bank online, and otherwise enter sensitive information online without third-party interference or interception when using the HTTPS internet protocol.

38. For example, users who log onto their e-trade.com brokerage accounts visit a web page secured by HTTPS. The information that users enter into their e-trade.com account remains private and can only be accessed by e-trade's servers.

39. On e-trade.com's web pages, the web address or "URL" in the browser sometimes reflects the e-trade.com user's brokerage account identification ("Account Id") -- e.g., <https://etws.etrade.com/accounts/rest/accountbalance/{AccountId}>. On a normally-functioning computer or Smartphone, this URL would not be accessible by third parties, and

1 thus does not pose a risk to the user of third-party interference or interception of the user's
2 brokerage Account Id. The portion of the URL that contains the Account Id would be encrypted
3 and therefore indecipherable by a third party.

4 40. However, IQ Agent can intercept HTTPS URLs and record them before they are
5 encrypted. In the example above, IQ Agent would capture the entire URL, including the
6 brokerage Account Id, despite the widely-held belief that online banking and trading is secure
7 due to the HTTPS protocol. Thus, IQ Agent functions similarly to a host of third-party malware
8 and nefarious software intended to steal passwords and other sensitive information.

9 41. The HTTPS protocol is not only used by Smartphone browsers. Smartphone
10 applications, such as applications available on the Android Marketplace, also may utilize the
11 HTTPS protocol to send and receive secure information. In such a situation, Carrier IQ again
12 captures the URL information despite its design as a secure protocol.

13 42. Therefore, because of its design and its interception of HTTPS URLs, IQ Agent
14 is systematically capturing and transmitting data to cellular carriers that is meant to be private
15 and is widely assumed to be private and inaccessible by third parties. Moreover, IQ Agent also
16 records details on applications usage. In particular, IQ Agent reports to cellular carriers which
17 applications users download and how much they use them.

18 **IV. Carrier IQ Enables Its Carrier Customers To Analyze Users' Information For Their**
19 **Own Purposes, Including For Marketing Purposes.**

20 43. The information captured by the IQ Agent software is transmitted to cellular
21 carriers either via storage on their web servers or on Carrier IQ's server. Carriers then use
22 Carrier IQ's proprietary web portal to access user information in a variety of ways.

23 44. For example, Carrier IQ's "IQ Insight Experience Manager" promises customers:
24 "IQ Insight enables you to align your business improvements with the things customers truly
25 value. Identify exactly how your customers interact with services and which ones they use. See
26 which content they consume, even offline."

27 45. Carrier IQ's "IQ Insight Experience Manager" provides its carrier customers with
28 "Actionable Intelligence" on their cell phone customers. Carrier IQ claims that its carrier

1 customers can use this intelligence to answer “business-critical questions, including: How long
2 does it take the user to start the service?” and “How do users respond to mobile advertising?”

3 46. Carrier IQ specifically advertises to its customers the ability to: “View
4 application and device feature usage, such as camera, music, messaging, browser and TV.”

5 47. In a press release issued June 8, 2011, Carrier IQ touted a recent marketing
6 analysis that it performed using its mobile intelligence tools: “In a recent operator rollout of
7 Carrier IQ’s application analytics, we were able to demonstrate that if Facebook was preloaded
8 on a specific smartphone, 40% of the app usage from that device in the first month was with
9 Facebook. Without the preload, it was only 5%, as users had to download the app themselves,”
10 said Andrew Coward, Vice President of Marketing at Carrier IQ.”

11 **V. The LG Defendants Install IQ Agent On Their Android Mobile Devices At The**
12 **Request Of Cellular Carriers And Without Users’ Knowledge Or Consent.**

13 48. Numerous cellular carriers, Android mobile device manufacturers, and Carrier IQ
14 have all confirmed that manufacturers alter the Android operating system code in order to
15 integrate IQ Agent at the request of cellular carriers.

16 49. The LG Defendants installed IQ Agent on Plaintiff’s Smartphone as well as
17 millions of other Android mobile devices at the request of cellular carriers.

18 50. The LG Defendants neither sought nor received the consent of mobile device
19 owners, including Plaintiff, to install IQ Agent on their mobile devices, and the LG Defendants
20 have never disclosed to mobile device owners, including Plaintiff, that IQ Agent is installed on
21 their mobile devices – much less the functions that IQ Agent performs.

22 **VI. Carrier IQ And Its Carrier Customers Claim That IQ Agent Is Secure And Does Not**
23 **Violate Consumer Privacy Interests.**

24 51. Carrier IQ and its carrier customers have strongly contested claims that IQ Agent
25 violates consumer expectations of privacy.

26 52. On its website, Carrier IQ claims that its technology encrypts and makes
27 anonymous the user information that it records and sends to its carrier customers.
28

1 53. In two public statements, Carrier IQ has claimed that IQ Agent does not record
2 keystrokes, provide its carrier customers with tracking tools, or report on the content of private
3 messages. Instead, Carrier IQ claims that its software produces secure, anonymous, aggregate
4 data for carriers and manufacturers to evaluate the performance of their hardware and networks.

5 54. Thus far, cellular carriers AT&T, Sprint and T-Mobile have confirmed that their
6 mobile devices integrate the IQ Agent software. Verizon Wireless, Research in Motion,
7 Microsoft and Nokia have denied that their mobile devices use the IQ Agent software. Apple
8 has stated that it formerly integrated IQ Agent into its iPhone but that it no longer does so.

9 55. All carriers and manufacturers who use IQ Agent have claimed that it is used
10 solely for the purpose of improving network performance and user experience. They have
11 denied that they receive or seek private information that is not anonymous or unidentifiable.

12 **VII. Carrier IQ's Claims Regarding The Security Of Its IQ Agent Software Are**
13 **Inaccurate And Misleading.**

14 56. The results of Trevor Eckhart's and Dan Rosenberg's independent investigations
15 into IQ Agent refute Carrier IQ's claims that its software is secure and does not violate
16 consumer privacy.

17 57. In particular, Eckhart and Rosenberg have demonstrated that IQ Agent does, in
18 fact, record various types of private information.

19 58. Eckhart's research also demonstrates that Carrier IQ utilizes its servers to record
20 information about users and their mobile devices. Most importantly, Eckhart demonstrates that
21 Carrier IQ's online portal for its customers identifies mobile devices by their equipment and
22 subscriber identification numbers, wholly refuting Carrier IQ's claim that its information is
23 transmitted anonymously.

24 59. Carrier IQ and its carrier customers have, in fact, confirmed that the information
25 recorded on users' mobile devices is transmitted both to Carrier IQ and to its carrier customers.

26 60. Carrier IQ has also confirmed that its products include a "customer care" solution
27 that offers cellular carriers the ability to gather information about particular mobile devices and
28 *identify the owners of those mobile devices* in order to provide them custom-tailored customer

1 care. Carrier IQ gives the example of carriers examining the applications downloaded and
2 websites visited by a user in order to inform the user whether those applications or websites are
3 over-utilizing the mobile device's system resources or battery.

4 61. Moreover, as to data that Carrier IQ does claim to transmit anonymously (where
5 the information stored in the HTTPS URLs captured by Carrier IQ contains identifying and
6 sensitive information such as passwords, names, addresses, and bank account numbers), Carrier
7 IQ's claims that such data is safe and does not violate consumer privacy are also inaccurate.

8 **PLAINTIFF'S ALLEGATIONS**

9 62. Plaintiff purchased his LG Marquee Smartphone from Sprint by means of an on-
10 line purchase through Sprint's website on September 27, 2011. Plaintiff activated his cellular
11 service with Sprint on his LG Marquee Smartphone in October of 2011.

12 63. Unbeknownst to Plaintiff at the time of his purchase, the LG Defendants had
13 altered the Google Android operating system on his Smartphone by installing IQ Agent on his
14 Smartphone.

15 64. Plaintiff first learned of IQ Agent on or about December 5, 2011 by reading about
16 the Carrier IQ cell phone tracking controversy on Yahoo's News website. Thereafter, Plaintiff
17 downloaded an application on his Smartphone called "Carrier IQ Detector". This application
18 purports to enable one to determine whether IQ Agent is installed on a Smartphone. According
19 to this application, IQ Agent is installed on Plaintiff's Smartphone.

20 65. Between October of 2011 and December of 2011, Plaintiff regularly used his LG
21 Marquee Smartphone to make calls, visit websites, send and receive emails, and download and
22 use applications. During this time, Plaintiff accessed and used numerous websites that are
23 secured by the HTTPS protocol.

24 66. By virtue of his regular use of his LG Marquee Smartphone on which the IQ
25 Agent software is installed, Plaintiff's private and personal communications have been illegally
26 intercepted and transmitted by Defendants.

CLASS ACTION ALLEGATIONS

67. This action is brought and properly may be maintained as a class action pursuant to the provisions of Fed.R.Civ.P. 23(a)(1)-(4) and 23(b)(1) or (b)(2) and satisfies the requirements thereof.

68. Plaintiff seeks to represent a nationwide class ("the Class") defined as follows: "All residents of the United States who presently own or have ever owned LG brand mobile devices on which IQ Agent is or was installed."

69. Plaintiff also seeks to represent a California resident subclass ("the California Subclass") defined as follows: "All residents of the State of California who presently own or have ever owned LG brand mobile devices on which IQ Agent is or was installed."

70. As used herein, the term "class members" shall mean and refer to the members of the Class and/or the California Subclass.

71. The class members are so numerous that joinder of all class members in one action is impractical. While the exact size of the classes and the identify of individual class members is unknown and cannot be ascertained without appropriate discovery, Plaintiff is informed and believes that the classes include millions of individual consumers.

72. There are questions of fact that are common to Plaintiff and the class members. These common questions, which do not vary among the class members, and which may be determined without reference to any class member's individual circumstances, include:

(a) Whether Carrier IQ designed and created the IQ Agent software for the purpose of intercepting and transmitting the class members' private wire and/or electronic communications and other electronic information;

(b) Whether the LG Defendants installed the IQ Agent software on their Android mobile devices;

(c) Whether Defendants intentionally intercepted the class members' wire and/or electronic communications; and

(d) Whether Defendants disclosed and/or used the class members' wire and/or electronic communications.

1 73. There are questions of law that are common to Plaintiff and the class members,
2 including:

3 (a) Whether the conduct of Defendants violated one or more of the
4 provisions of the Federal Wiretap Act, 18 U.S.C. § 2511 *et seq.*;

5 (b) Whether the conduct of Defendants has resulted in an actual controversy
6 such that declaratory relief is appropriate under the Declaratory Judgment Act, 28
7 U.S.C. §2201;

8 (c) Whether the conduct of Defendants constitutes an unfair business
9 practice in violation of California Business and Professions Code §17200;

10 (d) Whether the conduct of Defendants constitutes an unlawful business
11 practice in violation of California Business and Professions Code §17200; and

12 (e) Whether the conduct of Defendants constitutes an invasion of the class
13 members' privacy under California law.

14 74. The questions of law and fact that are common to the class members
15 predominate over the questions of law or fact, if any, that are individual to particular class
16 members.

17 75. Plaintiff's claims are typical of the claims of the class members. Defendants'
18 common course of conduct violated the Federal Wiretap Act and California law in the same
19 way and caused class members the same injuries. Likewise, Plaintiff and class members
20 must prove the same facts in order to establish Defendants' liability on the same claims.

21 76. Plaintiff will fairly and adequately represent and protect the interests of the
22 class members, and Plaintiff has no interests that are adverse to or that directly conflict with
23 those of the other class members.

24 77. Plaintiff has retained counsel who are experienced in litigation, including
25 complex class litigation, and who will zealously pursue the claims of the class members.

26 78. A class action is superior to all other available methods for the fair and efficient
27 adjudication of this controversy because the damages suffered by individual class members,
28 while not inconsequential, may be relatively small such that the expense and burden of

individual litigation make it economically unfeasible for the class members to initiate and pursue individual litigation in order to redress the wrongs done to them. Moreover, there will be no difficulty in the management of this case as a class action.

79. This action is certifiable under the provisions of Fed.R.Civ.P. 23(b)(1) and/or 23(b)(2) because:

(a) prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Defendants;

(b) prosecution of separate actions by individual class members would create a risk of adjudications as to them that would, as a practical matter, be dispositive of the interests of the other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

(c) Defendants have acted or refused to act on grounds generally applicable to the class members, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class members as a whole and necessitating that any such relief be applied on a class wide basis.

80. The class members are readily identifiable through records maintained by Defendants, and notice can be provided to the class members using methods and techniques (*e.g.* direct mail, publication, email, etc.) that have been accepted and approved by the courts for purposes of providing notice to class members in other nationwide class actions.

CLAIMS FOR RELIEF

First Claim For Relief

(Violation of the Federal Wiretap Act, 18 U.S.C. § 2511)

81. Plaintiff repeats and incorporates by reference paragraphs 1 through 80 above as if fully set forth herein.

82. Defendants intentionally intercepted or endeavored to intercept wire and/or electronic communications, both encrypted and unencrypted, of Plaintiff and the class members without their knowledge, authorization or consent in violation of 18 U.S.C. § 2511(a).

1 83. Defendants intentionally disclosed or endeavored to disclose to another person the
2 contents of wire and/or electronic communications, both encrypted and unencrypted, of Plaintiff
3 and the class members, knowing or having reason to know that the information was obtained
4 through the interception of wire and/or electronic communications, in violation of 18 U.S.C. §
5 2511(c).

6 84. Defendants intentionally used or endeavored to use the contents of wire and/or
7 electronic communications, both encrypted and unencrypted, of Plaintiff and the class members,
8 knowing or having reason to know that the information was obtained through the interception of
9 wire and/or electronic communications, in violation of 18 U.S.C. § 2511(d).

10 85. As a direct and proximate result of Defendants' violations of the Federal Wiretap
11 Act, Plaintiff and the class members have suffered harm due to the interception, disclosure and
12 use of their private information and communications.

13 86. Pursuant to 18 U.S.C. § 2520, Plaintiff and the class members are entitled to
14 statutory damages and other relief as follows:

15 (a) statutory damages in the maximum amount allowable;

16 (b) alternatively, to the extent they are greater than the maximum allowable
17 statutory damages, all profits made by Defendants as a result of the violations alleged
18 herein;

19 (c) punitive damages in an amount to be determined at trial, but in an
20 amount sufficient to prevent the same or similar conduct by Defendants in the future;
21 and

22 (d) reasonable attorneys' fees and other litigation costs reasonably incurred
23 by Plaintiff and the class members.

24 **Second Claim For Relief**

25 **(Declaratory Relief under the Declaratory Judgment Act, 28 U.S.C. § 2201)**

26 87. Plaintiff repeats and incorporates by reference paragraphs 1 through 80 above as if
27 fully set forth herein.
28

1 knowing or having reason to know that the information was obtained through the
2 interception of wire and/or electronic communications; and (c) intentionally using or
3 endeavoring to use the contents of wire and/or electronic communications, both encrypted
4 and unencrypted, of Plaintiff and the class members, knowing or having reason to know that
5 the information was obtained through the interception of wire and/or electronic
6 communications.

7 93. By engaging in these practices, Defendants have committed one or more acts of
8 unfair competition within the meaning of California Business and Professions Code § 17200,
9 *et seq.*

10 94. The practices engaged in by Defendants are unfair because they are immoral,
11 unethical, oppressive, unscrupulous and/or substantially injurious to Plaintiff and the class
12 members.

13 95. The practices engaged in by Defendants are unlawful because they violate the
14 Federal Wiretap Act, 18 U.S.C. § 2511(1)(a), (c) and/or (d) and because they constitute an
15 invasion of privacy.

16 96. Unless Defendants are enjoined from continuing to engage in these unfair and
17 unlawful business practices, Plaintiff and the class members will continue to be injured by
18 the wrongful actions and conduct of Defendants.

19 **Fourth Claim For Relief**

20 **(Invasion of Privacy)**

21 97. Plaintiff repeats and incorporates by reference paragraphs 1 through 80 above
22 as if fully set forth herein.

23 98. Without consent, Defendants intruded into the private communications,
24 conversations and matters of Plaintiff and the class members in a manner that would be
25 highly offensive to a reasonable person such as to constitute an invasion of privacy under
26 California law.

27 99. As a direct and proximate result of the actions and conduct of Defendants, the
28 privacy rights of Plaintiff and the class members have been invaded and violated.

1 100. Unless Defendants are enjoined from continuing to invade the privacy of
 2 Plaintiff and the class members, Plaintiff and the class members will continue to be injured
 3 by the wrongful actions and conduct of Defendants.

4 **PRAYER FOR RELIEF**

5 Plaintiff, on behalf of himself and the class members, prays for relief against
 6 Defendants as follows:

7 **On The First Claim For Relief**

8 For statutory damages in the maximum amount allowable;

9 Alternatively, to the extent they are greater than the maximum allowable statutory
 10 damages, for all profits made by Defendants as a result of the violations alleged herein;

11 For punitive damages in an amount to be determined at trial; and

12 For reasonable attorneys' fees and other litigation costs reasonably incurred by Plaintiff
 13 and the class members.

14 **On The Second Claim For Relief**

15 That this Court declare that that the practices engaged in by Defendants of (a)
 16 intentionally intercepting or endeavoring to intercept wire and/or electronic communications,
 17 both encrypted and unencrypted, of Plaintiff and the class members without their knowledge,
 18 authorization or consent, (b) intentionally disclosing or endeavoring to disclose to another
 19 person the contents of wire and/or electronic communications, both encrypted and
 20 unencrypted, of Plaintiff and the class members, knowing or having reason to know that the
 21 information was obtained through the interception of wire and/or electronic communications,
 22 and (c) intentionally using or endeavoring to use the contents of wire and/or electronic
 23 communications, both encrypted and unencrypted, of Plaintiff and the class members,
 24 knowing or having reason to know that the information was obtained through the
 25 interception of wire and/or electronic communications, are improper and unlawful.

26 **On The Third Claim For Relief**

27 For an order enjoining Defendants from (a) intercepting or endeavoring to intercept
 28 wire and/or electronic communications, both encrypted and unencrypted, of Plaintiff and the

1 class members without their knowledge, authorization or consent, (b) disclosing or
2 endeavoring to disclose to another person the contents of wire and/or electronic
3 communications, both encrypted and unencrypted, of Plaintiff and the class members, and (c)
4 using or endeavoring to use the contents of wire and/or electronic communications, both
5 encrypted and unencrypted, of Plaintiff and the class members;

6 For an order mandating the time and method of the disposal or destruction of the wire
7 and/or electronic communications intercepted by Defendants that belong to Plaintiff and the
8 class members; and

9 For an order mandating that the IQ Agent software be deactivated or removed from
10 all LG mobile devices or that all LG mobile devices installed with IQ Agent be replaced with
11 the same LG mobile devices without IQ Agent installed on them.

12 On The Fourth Claim For Relief

13 For an order enjoining Defendants from (a) intercepting or endeavoring to intercept
14 wire and/or electronic communications, both encrypted and unencrypted, of Plaintiff and the
15 class members without their knowledge, authorization or consent, (b) disclosing or
16 endeavoring to disclose to another person the contents of wire and/or electronic
17 communications, both encrypted and unencrypted, of Plaintiff and the class members, and (c)
18 using or endeavoring to use the contents of wire and/or electronic communications, both
19 encrypted and unencrypted, of Plaintiff and the class members;

20 For an order mandating the time and method of the disposal or destruction of the wire
21 and/or electronic communications intercepted by Defendants that belong to Plaintiff and the
22 class members; and

23 For an order mandating that the IQ Agent software be deactivated or removed from
24 all LG mobile devices or that all LG mobile devices installed with IQ Agent be replaced with
25 the same LG mobile devices without IQ Agent installed on them.

26 On All Claims For Relief

27 For all attorneys' fees, expenses and recoverable costs reasonably incurred in
28 connection with the commencement and prosecution of this action, provided that this action

1 results in the establishment and/or protection of the rights of the class members and/or
2 confers a substantial benefit on the class members; and

3 For such other and further relief as the Court deems just and proper.

4 **DEMAND FOR JURY TRIAL**

5 Plaintiff demands a trial by jury of all issues so triable in this action.

6 Dated: December 22, 2011

ARIAS OZZELLO & GIGNAC LLP

7
8 By:  _____

J. Paul Gignac, Esq.

10 FOLEY BEZEK BEHLE & CURTIS, LLP

11 Peter J. Bezek, Esq.

Robert A. Curtis, Esq.

12 Attorneys for Plaintiff
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28